WHAT IS CLAIMED IS:

1. An electronic seal, comprising:

an input/output section for receiving a random number encrypted based on a prescribed key; and

an advance authentication processing section for decrypting the encrypted and received random number based on a secret key related to the prescribed key and then encrypting the decrypted random number based on the secret key,

wherein the input/output section outputs the encrypted random number encrypted based on the secret key.

2. An electronic seal according to claim 1, wherein the advance authentication processing section includes:

a secret key memory section for storing the secret key;

a decryption section for decrypting the encrypted and received random number based on the secret key; and

an encryption section for encrypting the decrypted random number based on the secret key.

3. An electronic seal according to claim 1, further comprising a communication request section for outputting

a communication request ID, and the communication request section includes:

a memory section for storing the communication request ID; and

a reading section for reading the communication request ID from the memory section and outputting the communication request ID.

4. An electronic seal according to claim 1, wherein:

the random number encrypted based on the prescribed key is output from a memory medium, and

the input/output section is a reader/writer section for supplying a power to the memory medium.

5. An electronic seal according to claim 1, wherein:

the prescribed key is a public key, and

the secret key forms a key pair with the public key based on one of an RSA cryptosystem and an elliptic curve cryptosystem.

6. An electronic seal according to claim 1, further comprising:

a display section for displaying at least a mode menu and a mode execution result;

a selection key for selecting a prescribed mode from a plurality of modes;

a determination key for determining on the selected mode;

a numeral setting key for setting a numerical value; and

a start key for starting execution of the determined mode.

7. An electronic seal according to claim 6, wherein an external shape of the electronic seal is one of a card-shape, a cylindrical shape, and a prism shape.

8. An electronic seal according to claim 1, further comprising:

an initial setting mode section for receiving key information including the prescribed key and the secret key from an external device only once and retaining the key information; and

a registered seal mode section for outputting the prescribed key.

9. An electronic seal according to claim 1, further comprising a cancel mode section for canceling a result

of advance authentication based on an operation of the advance authentication processing section.

10. An electronic seal according to claim 1, further comprising a period setting mode section for outputting information representing an expiration time of a valid time period of use to an external device.

11. An electronic seal according to claim 1, further comprising a times setting mode section for outputting information representing a valid number of times of use to an external device.

12. An electronic seal according to claim 1, further comprising a sum setting mode section for outputting information representing an upper limit of a sum which can be spent in one transaction to an external device.

13. An electronic seal according to claim 6, further comprising a clock mode section for displaying the current time on the display section.

14. A memory medium, comprising:

an advance authentication processing section for

generating a random number, encrypting the generated random number based on a prescribed key, decrypting a random number, encrypted based on a secret key related to the prescribed key, based on the prescribed key, and comparing the generated random number and the decrypted random number; and

an input/output section for outputting the random number encrypted based on the prescribed key and receiving the random number encrypted based on the secret key.

15. A memory medium according to claim 14, wherein the advance authentication processing section includes:

a random number generation section for generating the random number;

a prescribed key memory section for storing the prescribed key;

an encryption section for encrypting the generated random number based on the prescribed key;

a decryption section for decrypting the random number, encrypted based on the secret key, based on the prescribed key;

a random number comparison section for comparing the generated random number and the decrypted random number; and

a comparison result memory section for storing a result of comparison.

16. A memory medium according to claim 14, further comprising a start signal generation section for generating a start signal based on a communication request ID, wherein the start signal generation section includes:

a communication request ID memory section for storing the communication request ID; and

a communication request ID comparison section for comparing a communication request ID which is input from an external device and the communication request ID stored in the communication request ID memory section,

wherein the communication request ID comparison section outputs the start signal when the input communication request ID and the communication request ID stored in the communication request ID memory section match each other.

17. A memory medium according to claim 16, wherein the input/output section receives the communication request ID from the external device.

18. A memory medium according to claim 14, wherein:

the prescribed key is a public key, and

the secret key forms a key pair with the public key based on one of an RSA cryptosystem and an elliptic curve cryptosystem.

19. A memory medium according to claim 15, further comprising an access permission processing section for permitting an access when the result of comparison indicates that the generated random number and the decrypted random number match each other, and for prohibiting an access when the result of comparison indicates that the generated random number and the decrypted random number do not match each other.

20. A memory medium according to claim 19, wherein, when the result of comparison indicates that the generated random number and the decrypted random number match each other, the access permission processing section permits an access and resets the result of comparison stored in the comparison result memory section.

21. A memory medium according to claim 14, further comprising an initial setting mode section for setting a prescribed key which is input from an external device.

22. A memory medium according to claim 21, further comprising a prescribed memory section, wherein the initial setting mode section outputs the input prescribed key to the prescribed key memory section.

23. A memory medium according to claim 14, further comprising a cancel mode section for canceling a result of advance authentication based on an operation of the advance authentication processing section.

24. A memory medium according to claim 14, further comprising a period setting mode section for prohibiting an access after an expiration time of a valid time period of use has passed.

25. A memory medium according to claim 14, further comprising a times setting mode section for prohibiting an access when a number of times that the memory medium has been used exceeds a valid number of times of use.

26. A memory medium according to claim 14, further comprising a sum setting mode section for prohibiting an access when a sum to be used exceeds an upper limit of

a sum which can be spent in one transaction.

27. An advance authentication system, comprising a memory medium and an electronic seal,

wherein the memory medium includes:

a first advance authentication processing section for generating a random number and encrypting the generated random number based on a prescribed key, and

a first input/output section for outputting the random number encrypted based on the prescribed key, and

wherein the electronic seal includes:

a second input/output section for receiving the random number encrypted based on the prescribed key, and

a second advance authentication processing section for decrypting the encrypted and received random number based on a secret key related to the prescribed key and then encrypting the decrypted random number based on the secret key,

wherein:

the second input/output section outputs the random number encrypted based on the secret key,

the first input/output section receives the random number encrypted based on the secret key,

the first advance authentication processing

section decrypts the random number, encrypted based on the secret key, based on the prescribed key, and compares the generated random number and the random number decrypted based on the prescribed key, and

the memory medium and the electronic seal perform mutual data communication to perform advance authentication processing.

28. An advance authentication system according to claim 27, wherein the memory medium is one of an IC card and a memory card.

29. A mobile device including an electronic seal, wherein the electronic seal includes:

an input/output section for receiving a random number encrypted based on a prescribed key; and

an advance authentication processing section for decrypting the encrypted and received random number based on a secret key related to the prescribed key and then encrypting the decrypted random number based on the secret key,

wherein the input/output section outputs the encrypted random number encrypted based on the secret key.

30. A mobile device according to claim 29, wherein the mobile device is a cellular phone detachably accommodating the electronic seal.

31. A vehicle start control apparatus including a memory medium, wherein the memory medium includes:

an advance authentication processing section for generating a random number, encrypting the generated random number based on a prescribed key, decrypting a random number, encrypted based on a secret key related to the prescribed key, based on the prescribed key, and comparing the generated random number and the decrypted random number; and

an input/output section for outputting the random number encrypted based on the prescribed key and receiving the random number encrypted based on the secret key.